

Accton

Making Partnership Work

Cheetah Wireless™ 802.11a Access Point - WA5001

Quick Installation Guide



Accton

Making Partnership Work

Quick Installation Guide

Cheetah Wireless™ 802.11a Access Point

802.11a Wireless Access Point

with 1 10/100Mbps (RJ-45) LAN Port



Copyright © 2003 by Accton Technology Corporation. All rights reserved.

No part of this document may be copied or reproduced in any form or by any means without the prior written consent of Accton Technology Corporation.

Accton makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. Accton reserves the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

Accton

International Headquarters

No. 1 Creation Road III,
Science-based Industrial Park
Hsinchu 300, Taiwan, R.O.C.
Phone: +886-3-5770-270
Fax: +886-3-5770-267
Internet: support@accton.com.tw

Europe Headquarters

Edificio Conata II,
Calle Frutuós Gelabert 6-8, 2^a, 4^a,
08970 - Sant Joan Despí,
Barcelona, Spain.
Phone: +34-93-477-4920
Fax: +34-93-477-3774

Asia Pacific Headquarters

1 Claymore Drive
#08-05/06 Orchard Towers (Rear Block)
Singapore 229594
Phone: +65 238 6556
Fax: +65 238 6466
Internet: www.acctontech.com

Accton is a trademark of Accton Technology Corporation. Other trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective companies.

WA5001
E042003-R01
150000007000A

Accton Technology Corporation

Limited Warranty: Accton warrants all its products to be free of manufacturing defects in workmanship and materials, under normal use and service, for the applicable warranty term. All Accton products carry a standard 90-day limited warranty from the date of purchase from Accton or its Authorized Reseller. Accton may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from Accton or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the Accton web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an 'Active' Accton product. A product is considered to be 'Active' while it is listed on the current Accton price list. As new technologies emerge, older technologies become obsolete and Accton will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an 'Active' Accton product. A list of discontinued products is attached with the most recent version being available on the support section of our web site (<http://www.acctontech.com>).

All products that are replaced become the property of Accton. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. Accton is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to Accton pursuant to any warranty. Products returned to Accton should have any customer -installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. Accton is not responsible for these items if they are returned with the product.

Customers must contact Accton for a Return Material Authorization number prior to returning any product to Accton. Proof of purchase may be required. Any product returned to Accton without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. Customers are responsible for all shipping charges from their facility to Accton. Accton is responsible for return shipping charges from Accton to customer.

Limited Warranty

WARRANTIES EXCLUSIVE: IF AN ACCTON PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT ACCTON'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ACCTON NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. ACCTON SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL ACCTON BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF ACCTON OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME COUNTRIES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* Accton will provide warranty service for up to three years following discontinuance from the active Accton price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one -year warranty from date of purchase.

Contents

Introduction	1
Package Checklist	1
System Requirements	1
Hardware Description	2
Ethernet Compatibility	2
Radio Characteristics	2
LED Indicators	2
Applications	3
Hardware Installation	4
Software Installation and Configuration	6
Windows Installation (98/Me/NT/2000/XP)	6
Setup Wizard	7
Advanced Setup	11
Identification	12
Channel	12
Performance	13
Synchronization	14
Transmit Threshold	15
TCP / IP Settings	16
Encryption	17
Authentication Type	18
Standard WEP Setup (WEP Default: Disable)	18
Advanced WEP Setup	18
SNMP	19
System	20
Administration	20
Factory Default	20
Upgrade Firmware	20
Status	21
Access Point Status	21
AP Configuration	22
AP SME (Station Management Entity)	22
AP Statistics	22
Connected Station Status	22
Station Configuration	23
Station SME	23
Station Statistics	23

Network Configuration and Planning	24
Network Topologies	24
Ad Hoc Wireless LAN (no AP or Bridge)	24
Infrastructure Wireless LAN	25
Infrastructure Wireless LAN for Roaming Wireless PCs	26
Troubleshooting	27
Accton Networks	27
Specifications	28
Terminology	31

Introduction

Accton's Cheetah Wireless 802.11a Access Point (WA5001) provides transparent, wireless high speed data communications for portable or mobile devices equipped with an 802.11a wireless adapter (such as the WN5301). These communications can be between the access point and the wired LAN, between the access point and the wireless network, or within the wireless network.

This offers fast, reliable wireless connectivity with considerable cost savings over wired LANs (which include long-term maintenance overhead for cabling). Using this 802.11a technology, the access point can easily integrate with the existing 10/100 Ethernet LAN.

Package Checklist

The Cheetah Wireless 802.11a Access Point package includes:

- One Cheetah Wireless Access Point (WA5001)
- One 3.3 V DC power adapter
- One installation CD-ROM which includes the User Guide and the 802.11a Utility Program
- This Quick Installation Guide

Please complete the warranty registration card and return to Accton or register online at: **register.acctontech.com**.

Please inform your dealer if there are any incorrect, missing or damaged parts. If possible, retain the carton, including the original packing materials. Use them again to repack the product if there is a need to return it for repair.

System Requirements

Before you install the Wireless Access Point, be sure you meet the following requirements:

- An A/C power outlet (100~240 V, 50~60 Hz) which will supply power for the access point
- An available RJ-45 (UTP) port on a 10/100 Mbps Ethernet hub or switch
- 802.11a compliant wireless Ethernet adapters with TCP/IP compatible protocol installed
- Web browser for configuration

Hardware Description

Ethernet Compatibility

Accton's Wireless Access Point can attach directly to 10BASE-T/100BASE-TX (twisted-pair) Ethernet LAN segments. These segments must conform to the IEEE 802.3 specification.

The access point appears as an Ethernet node and performs a routing function by moving packets from the wired LAN to remote workstations on the wireless infrastructure.

Radio Characteristics

The Wireless Access Point uses a radio modulation technique known as Orthogonal Frequency Division Multiplexing (OFDM), and a shared collision domain (CSMA/CA). It operates at the 5 GHz Unlicensed National Information Infrastructure (UNII) band with turbo mode. Data is transmitted over a half-duplex radio channel operating at up to 72 Megabits per second (Mbps) in the turbo mode, and with a maximum operating range up to 500 m (1650 feet).

LED Indicators

The Wireless Access Point includes three status LED indicators, as described in the following figure and table.

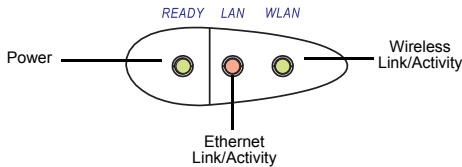


Figure 1. Status LEDs

LED	Status	Description
Power	On	Indicates that power is being supplied.
	Flashing	Indicates: <ul style="list-style-type: none"> • running a self-test • loading software program • system errors (See "Troubleshooting" on page 27)
Ethernet Link/Activity (Green)	On	Indicates a valid 100 Mbps Ethernet cable link.
	Flashing	Indicates that the access point is transmitting or receiving data on the 100 Mbps Ethernet LAN. The flashing rate is proportional to your network activity.

LED	Status	Description
Ethernet Link/ Activity (Amber)	On	Indicates a valid 10 Mbps Ethernet cable link.
	Flashing	Indicates that the access point is transmitting or receiving data on the 10 Mbps Ethernet LAN. The flashing rate is proportional to your network activity.
Wireless Link/ Activity	On	Indicates a valid wireless link.

Applications

The Cheetah Wireless products offer a high speed, reliable, cost-effective solution for 10/100 Mbps wireless Ethernet client access to the network in applications such as:

- **Remote access to corporate network information**
E-mail, file transfer and terminal emulation
- **Difficult-to-wire environments**
Historical or old buildings, asbestos installations, and open areas where wiring is difficult to employ
- **Frequently changing environments**
Retailers, manufacturers, and banks which frequently rearrange the workplace or change location
- **Temporary LANs for special projects or peak times**
Trade shows, exhibitions, and construction sites which need temporary setup for a short time period. Retailers, airline and shipping companies which need additional workstations for a peak period. Auditors who require workgroups at customer sites.
- **Access to databases for mobile workers**
Doctors, nurses, retailers, or mobile workers who need access to databases while being mobile in a hospital, retail store or an office campus.
- **SOHO (Small Office and Home Office)**
SOHO users who need easy and quick installation of a small computer network.

Hardware Installation



Figure 2. Top Panel

1. **Select the Site** — Choose a proper place for your WA5001 Wireless Access Point. In general, the best location is at the center of your wireless coverage area, within line of sight of all wireless devices.
2. **Placement of the Wireless Access Point** — Proper placement will improve performance. Try to place the access point in a position that can best cover its BSS (page 25). Normally, the higher you place the antenna, the better the performance.

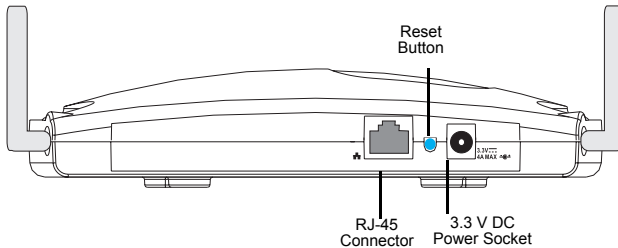


Figure 3. Rear Panel

3. **Connect the Ethernet Cable** — The WA5001 can be wired to a 10/100 Mbps Ethernet through a network device such as a hub or a switch. Connect to the RJ-45 connector socket on the back panel with category 3, 4 or 5 UTP Ethernet cable and an RJ-45 connector.

4. **Connect the Power Cable** — Connect the power adapter cable to the 3.3 V DC power socket on the rear panel.

Warning: USE ONLY the power adapter supplied with the WA5001. Otherwise, the product may be damaged.

The CD-ROM that comes with the package contains a utility program for the access point. Any updates can be downloaded from Accton's Web site at:

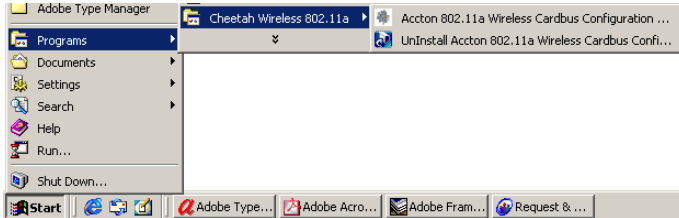
<http://www.acctontech.com>.

The WA5001 can be configured over an Ethernet network using RJ-45 cable. You may connect the WA5001 to a network device such as a hub or switch. Then, run the utility program, and configure the WA5001 remotely, as described on the next page.

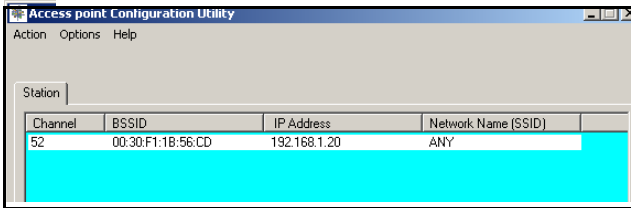
Software Installation and Configuration

Windows Installation (98/Me/NT/2000/XP)

1. Insert the CD-ROM that comes with the package into the CD-ROM drive on your PC, and then enter the following command: D:\utility\setup. Follow the on-screen instructions to install the utility program.
2. After you finish the installed utility, choose Programs from the Start menu. Then select Cheetah Wireless 802.11a, and the configuration utility.



3. The program will then detect all the WA5001 Wireless Access Point(s) on the network. (Default WA5001 IP address is 192.168.1.20)



4. If DHCP is turned ON (the default setting is Disable, page 16) and a DHCP server is located on the network, then the access point will automatically be assigned an IP address when booted. From the list of detected devices (see the above screen), select and double-click on the unit you want to configure.
5. The Web management window will appear. You can also manually launch a web browser from a PC and enter the IP address that is assigned to the WA5001. The WA5001 802.11a AP Web-based configuration page will be displayed.

Setup Wizard

1. To view the access point's management interface, enter the user name Admin, with a password 5up, and click LOGIN.

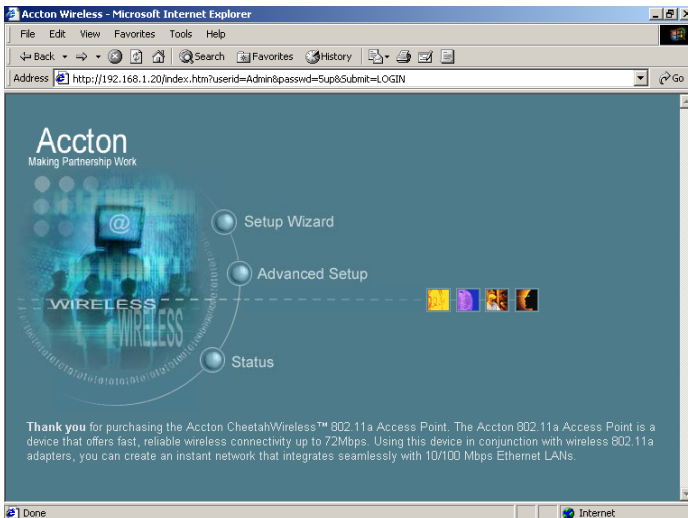
LOGIN USER ID & PASSWORD

Username:

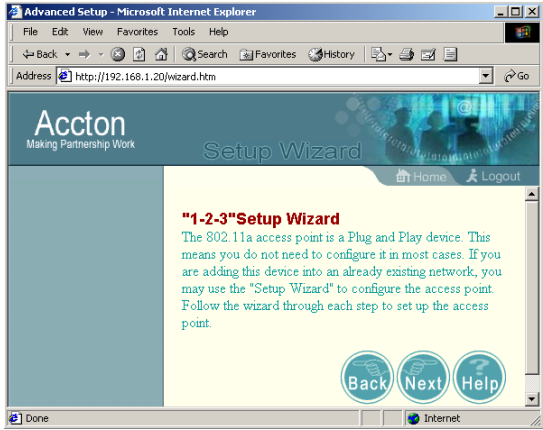
Password:

Please enter Username and Password.

2. The home page displays the Main Menu on the screen.
3. Click on Setup Wizard to display basic configurations including SSID, Channel, Authentication Type and Standard WEP Setup.

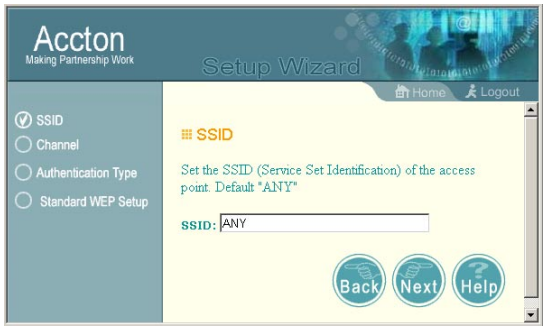


4. Click on the Next button to start using the 1-2-3 Setup Wizard.



SSID — The Service Set ID. This should be set to the same value as other wireless devices in your network. (Default: ANY)

Note: The SSID is case sensitive and can consist of up to 32 alphanumeric characters.



Channel — You can select Enable to set the access point to operate in turbo mode with a data rate of up to 72 Mbps. (Default: Disable)

The screenshot shows the 'Channel' configuration screen in the Accton Setup Wizard. The left sidebar has 'Channel' selected. The main area shows 'Turbo Mode' with 'Disable' selected and 'Enable' as an option. There are 'Back', 'Next', and 'Help' buttons at the bottom.

Authentication Type – Check the Shared Key radio button to start filtering frames with addresses defined in the Standard WEP Setup screen. (Default: Open System)

The screenshot shows the 'Authentication Type' configuration screen. The left sidebar has 'Authentication Type' selected. The main area shows 'Open System' selected and 'Shared Key' as an option. There are 'Back', 'Next', and 'Help' buttons at the bottom.

Standard WEP Setup — For more secure data transmission, check the Enable radio button to ensure wireless network security. Then select one shared key (1 ~ 4) and the proper key size. (WEP Default: Disable)

The screenshot shows the 'Standard WEP Setup' configuration screen. The left sidebar has 'Standard WEP Setup' selected. The main area shows 'WEP' with 'Enable WEP' selected and 'Default Shared Key' with options 1, 2, 3, and 4. Below is a table for shared keys and key sizes, and 'Back', 'Finish', and 'Help' buttons at the bottom.

Shared Key	Encryption Key	Key Size
Shared Key 1:	<input type="text"/>	64 bit
Shared Key 2:	<input type="text"/>	64 bit
Shared Key 3:	<input type="text"/>	64 bit
Shared Key 4:	<input type="text"/>	64 bit

Quick Installation Guide

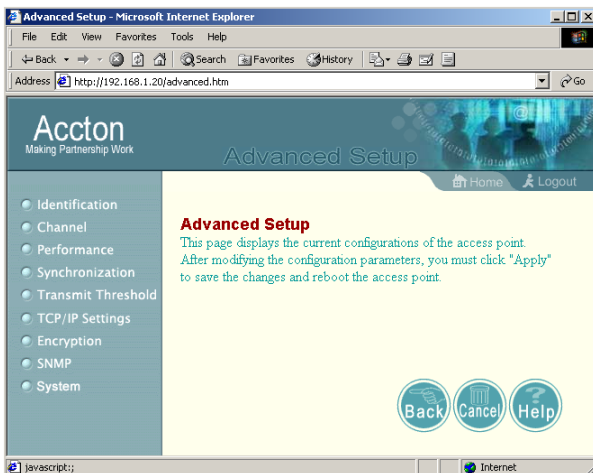
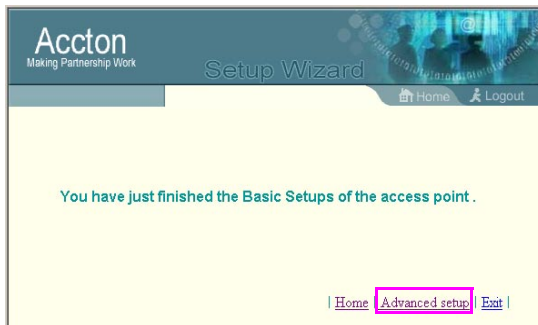
Wired Equivalent Privacy (WEP) is implemented in this device to prevent unauthorized access to your wireless network. All wireless devices must have the same Key ID to communicate.

Key Length (Manual Entry)	Hex Digits per Key ID
64-bit: supports 4 shared keys	10 HEX digits
128-bit: supports 1 shared key	26 HEX digits
152-bit: supports 1 shared key	32 HEX digits

5. Click on the Finish button when completed.

Advanced Setup

Click the Advanced setup in the bottom right-hand corner to display additional information about the access point configuration as shown below:



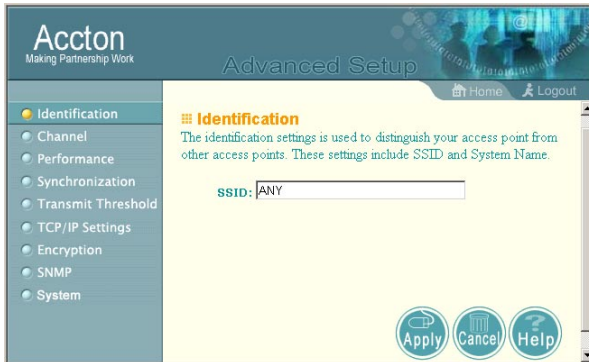
Note: The Advanced Setup screen allows you to view and change the current configuration of the access point. After modifying the configuration parameters, you must click on the Apply button to save the changes. The new settings will not take effect until you click Apply to refresh the access point. Then you need to click the Reboot button to reboot the access point. The Web browser loses connectivity with the AP Web server when the access point reboots. To establish a network connection to the rebooted access point, wait until it has finished rebooting.



Identification

The SSID (Service Set Identification) is the name of a basic service set provided by an access point. All clients that want to connect to the Internet via an access point must set their SSIDs to the same as that of the access point.

SSID: This should be set to the same value as other wireless devices in your network. (Default: ANY).



Channel



Radio Channel: The radio channel through which the access point communicates to PCs in its BSS (page 25). Note that the radio channel for wireless clients is automatically set to the same as that used by the access point to which it is linked. (Default: 52 for US and 38 for Japan)

Note: The available channel settings are limited to local regulations, which determine the number of channels that are available.

- FCC: 8 channels
- MKK: 5 channels

Turbo Mode: You may either Enable or Disable the Turbo Mode. (Default: Disable)

Turbo Mode is the enhanced wireless LAN operating mode (not regulated in the standard IEEE 802.11a) that can provide a higher data rate. The Normal Mode of the 802.11a access point provides connections up to 54 Mbps. Enabling Turbo Mode on the 802.11a access point allows the access point to provide connections with a data rate of up to 72 Mbps.

Note: In Normal Mode, the channel bandwidth is 20 MHz. In Turbo Mode, the channel bandwidth is increased to 40 MHz. However, there are only three channels available when the Turbo Mode is enabled (only 1 channel in Japan).

Performance

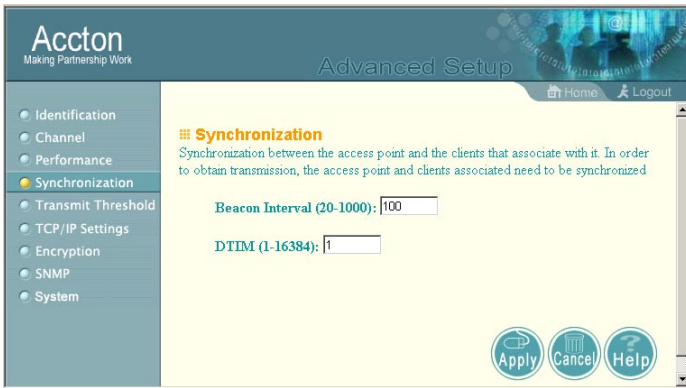


Data Rate: Select “best” from the drop-down list to optimize the data transfer speed for your network. (Default: best)

Transmit Power: Set the signal strength transmitted from the access point. The longer the transmission distance, the higher the transmission power required. (Default: full)

Synchronization

In order to obtain transmission, the access point and connected clients need to be synchronized



Beacon Interval (20-1000 K μ s): Set the beacon interval between synchronization frames. These synchronization frames may also contain an indication of frames that are to be transmitted to stations in Power Save mode. (Default: 100)

Note: 1K μ s = 1000 microsecs = 1 ms

DTIM (1-16384): Set the Delivery Traffic Indication Message (DTIM) interval. The DTIM indicates how often the MAC layer forwards multicast traffic. This parameter is necessary to accommodate stations using Power Save mode. In order to maximize the utilization of channels, broadcast data is not transmitted after every beacon interval for stations in Power Save mode. These stations must wake up to receive broadcast data at the DTIM interval.

The DTIM is the interval between two synchronization frames with broadcast information. If you set the value to 2, the access point will save all multicast frames for the BSS and forward them after every second beacon interval. Smaller DTIM intervals deliver multicast frames more frequently, causing stations in Power Save mode to wake up more often and drain power faster. Higher DTIM intervals delay the transmission of multicast frames. (Default: 1)

Transmit Threshold

The screenshot shows the Accton Advanced Setup web interface. The header includes the Accton logo with the tagline "Making Partnership Work" and the page title "Advanced Setup". A navigation menu on the left lists various configuration categories: Identification, Channel, Performance, Synchronization, Transmit Threshold (highlighted with a yellow dot), TCP/IP Settings, Encryption, SNMP, and System. The main content area is titled "Transmit Threshold" and contains the following text: "Set the Transmit Threshold. In this page you may set the Fragment Length and the RTS Length." Below this text are two input fields: "Fragment Length (256-2346):" with a text box containing "2346", and "RTS Length (256-2346):" with a text box containing "2346". At the bottom right of the form are three buttons: "Apply", "Cancel", and "Help".

Fragment Length (256-2346): The Fragment Length can be set between 256 and 2,346. If the packet size is smaller than the preset fragment size, the packet will not be segmented.

Fragmentation of the packets can increase the reliability of transmission because it increases the probability of a successful transmission due to smaller frame size. If there is significant interference present or collisions due to high network utilization, try setting the fragment size to a smaller value. This will enable the retransmission of smaller frames much faster. However, it is more efficient to set a longer fragment length if very little or no interference is present because there are overhead costs in sending multiple frames. (Default: 2346)

RTS Length (256-2346): Set the RTS (Request to Send) frame length.

You may configure the access point to initiate an RTS frame sequence always, never, or only for frames longer than a specified length. If the packet size is smaller than the preset RTS threshold size, the RTS/CTS mechanism will NOT be enabled

The access point sends request to send (RTS) frames to a particular receiving station to negotiate the transmission of a data frame. After receiving an RTS, the station sends a CTS (Clear to Send) frame to acknowledge the right for the sending station to transmit data frames. Access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node Problem." (Default: 2346)

TCP / IP Settings



Set the TCP/IP configuration for accessing the Internet.

DHCP Client: If Enable is selected, the IP address, subnet mask and default gateway can be dynamically assigned to the access point by the network DHCP server. (Default: Disable)

Note: If there is no DHCP server on your network, then the access point will automatically start up with its default IP address, 192.168.1.20.

By using the Wireless Access Point's built-in DHCP (Dynamic Host Configuration Protocol) server, you are allowing the Wireless Access Point to handle all the IP addressing on your Local Area Network (LAN). This can save you much of the time and hassle of setting up your network.

DHCP Server: If you have a server on your network that requires a static IP address, select Enable under DHCP Server and then manually assign a static IP address to your server. (Default: Disable)

Encryption

For more secure data transmission, you may enable WEP (Wired Equivalent Privacy) to prevent unauthorized access to your wireless network. The WEP setting must be the same for each client in your wireless network.

Accton
Making Partnership Work

Advanced Setup

[Home](#) [Logout](#)

- [Identification](#)
- [Channel](#)
- [Performance](#)
- [Synchronization](#)
- [Transmit Threshold](#)
- [TCP/IP Settings](#)
- [Encryption](#)
- [SNMP](#)
- [System](#)

Encryption

You may set the Wired Equivalency Privacy (WEP) configurations of the access point.

Authentication Type
 Open System Shared Key

Standard WEP Setup

For 64 bit WEP, enter 10 hexadecimal digits
 For 128 bit WEP, enter 26 hexadecimal digits
 For 152 bit WEP, enter 32 hexadecimal digits

- WEP: Disable Enable WEP
- Default Shared Key: 1 2 3 4

Shared Key	Encryption Key	Key Size
Shared Key 1:	<input type="text"/>	64 bit ▼
Shared Key 2:	<input type="text"/>	64 bit ▼
Shared Key 3:	<input type="text"/>	64 bit ▼
Shared Key 4:	<input type="text"/>	64 bit ▼

Advanced WEP Setup
 In addition to the standard WEP key, 60 per station unique keys also supported. You may add the unique key ID which starts from 5 and ends at 64.

Access Control List Setup
 Set the MAC Address Filter

Unique Key	Encryption Key	Key Size
5 ▼	<input type="text"/>	64 bit ▼
<input checked="" type="radio"/> Read <input type="radio"/> Write <input type="radio"/> Delete		

ACL: Disable Enable Strict

ACL Id:	MAC Address	Key Map	permission
0	<input type="text"/>	0	<input type="radio"/> Deny <input checked="" type="radio"/> Allow
<input checked="" type="radio"/> Read <input type="radio"/> Write <input type="radio"/> Delete			

Apply
 Cancel
 Help

Authentication Type

You may choose either the Open System or the Shared Key. (Default: Open System)

If Shared Key is enabled, WEP should be enabled and at least one shared key should be defined. But you can enable WEP, and set the authentication type as Open System.

Standard WEP Setup (WEP Default: Disable)

Default Shared Key— Choose the Shared Key that has the encryption string you prefer (Key 1~4 for 64-bit).

Note: All wireless devices must have the same Key ID values to communicate.

Key Length (Manual Entry)	Hex Digits per Key ID
64-bit: supports 4 shared keys	10 HEX digits
128-bit: supports 1 shared key	26 HEX digits
152-bit: supports 1 shared key	32 HEX digits

Advanced WEP Setup

How to set up the Unique Key WEP:

1. Select a unique key (5 ~ 64)
2. Enter the encryption key and select the proper key size.
3. Click Write and Apply to save the encryption key.
4. If you want to read an encryption key, select the unique key you want to read, then click Read and Apply to view the encryption key.
5. If you want to delete an encryption key, select the unique key you want to delete, click Delete and Apply to delete the encryption key.

Using Access Control List

Set the Access Control List (ACL) to filter out specified MAC addresses. The ACL provides a mechanism to take certain actions based on the stations MAC address. Any frames with a source or destination MAC address entered in this table will be filtered from the access point.

How to Set up the Access Control List:

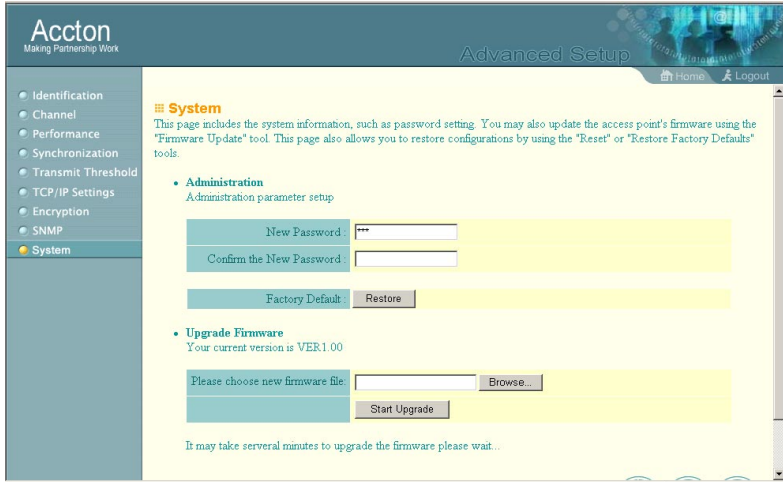
1. Select ACL Enable
2. Enter an ACL ID (1 ~ 60)
3. Enter the MAC address of the station you want to set up.
4. Enter a Key Map, one of the shared keys (1 ~ 4) or one of the unique keys (5 ~ 64), and choose Allow or Deny. If the station's WEP key is the same as the Key Map you assigned, the station will then allow or deny connections to the access point.
5. If you just enable the ACL, all stations that have shared keys can also connect to the access point. If you set the ACL to Strict, only stations with MAC addresses in the ACL can connect to the access point.

SNMP



Use this screen to display and enter a community string for the Simple Network Management Protocol (SNMP). To communicate with the access point, the SNMP agent must first be enabled, and the Network Management Station must submit a valid community string for authentication.

System



Administration

New Password

Change the access point's password.

Factory Default

Use the Restore button to load the factory default configuration and reboot this device. Note that all user-configured information will be lost. You will also have to re-enter the password to regain management access to this device.

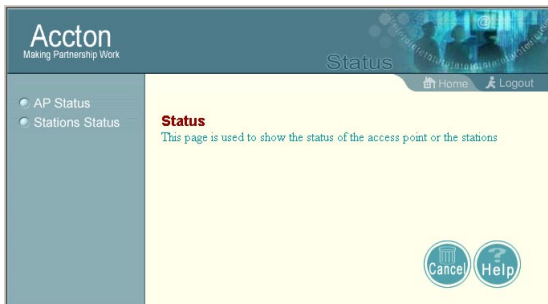
Upgrade Firmware

Click Browse to locate the downloaded firmware file and press Start Upgrade to start the upgrade process.

For the latest firmware version information, visit Accton's Web site at:

www.acctontech.com

Status



Checking the AP Status and Stations Status radio buttons on the home page displays additional information about the access point status and Stations Status as shown in the following section:

Access Point Status

AP Configuration

MAC Address	0030F11E56CD
State	up
TransState	0
Channel	52
Turbo Mode	OFF
WEP	OFF
Authentication Type	Open System
Power Save Mode	OFF
RcvRate	0

AP SME

State	up
Authentication Type	Open System
Authentications	0
Associations	0

AP Statistics

AckSignalStrength	0	RcvSignalStrength	0
TxDragments	601172	RxDragments	0
TxDDataFrames	601164	RxDDataFrames	0
TxDMgmtFrames	22	RxDMgmtFrames	0
TxDMulticastFrames	601175	RxDMulticastFrames	0
TxDMultiLongFrameRetries	0	FerRetCnt	0

Quick Installation Guide

In the AP Status page, click the appropriate hyperlink to view the access point configuration, access point SME statistics (station association information), or access point (transmit and receive) statistics.

AP Configuration

View the access point configuration

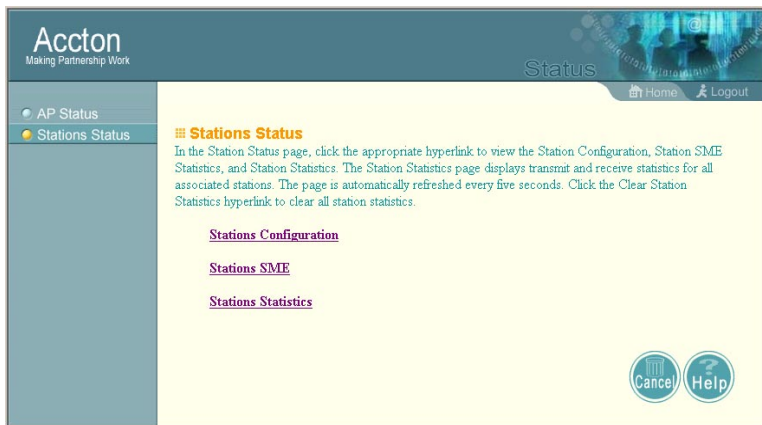
AP SME (Station Management Entity)

View the station association information

AP Statistics

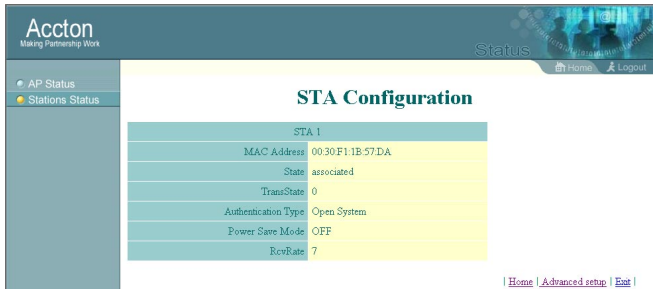
View transmit and receive statistics

Connected Station Status



In the Stations Status page, click the appropriate hyperlink to view the Station Configuration, Station SME statistics, and Station Statistics. The Station Statistics page displays transmit and receive statistics for all associated stations. The page is automatically refreshed every five seconds.

Station Configuration

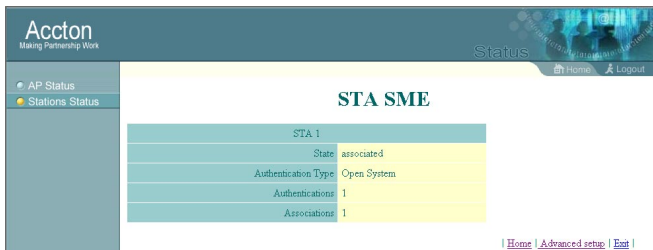


The screenshot shows the 'STA Configuration' page in the Accton web interface. The page title is 'STA Configuration'. The left sidebar has 'AP Status' and 'Stations Status' (selected). The main content area displays configuration details for 'STA 1' in a table format. At the bottom right, there are links for 'Home', 'Advanced setup', and 'Exit'.

STA 1	
MAC Address	0030F11E57DA
State	associated
TransState	0
Authentication Type	Open System
Power Save Mode	OFF
RecvRate	7

| [Home](#) | [Advanced setup](#) | [Exit](#) |

Station SME

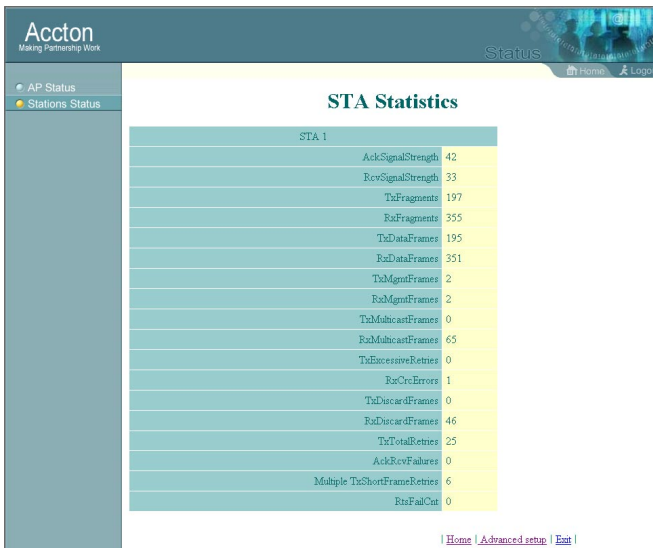


The screenshot shows the 'STA SME' page in the Accton web interface. The page title is 'STA SME'. The left sidebar has 'AP Status' and 'Stations Status' (selected). The main content area displays SME details for 'STA 1' in a table format. At the bottom right, there are links for 'Home', 'Advanced setup', and 'Exit'.

STA 1	
State	associated
Authentication Type	Open System
Authentications	1
Associations	1

| [Home](#) | [Advanced setup](#) | [Exit](#) |

Station Statistics



The screenshot shows the 'STA Statistics' page in the Accton web interface. The page title is 'STA Statistics'. The left sidebar has 'AP Status' and 'Stations Status' (selected). The main content area displays statistics for 'STA 1' in a table format. At the bottom right, there are links for 'Home', 'Advanced setup', and 'Exit'.

STA 1	
AckSignalStrength	42
RecvSignalStrength	33
TxFragments	197
RxFragments	355
TxDataFrames	195
RxDataFrames	351
TxMgmtFrames	2
RxMgmtFrames	2
TxMulticastFrames	0
RxMulticastFrames	65
TxExcessiveRetries	0
RxCrcErrors	1
TxDiscardFrames	0
RxDiscardFrames	46
TxTotalRetries	25
AckRecvFailures	0
Multiple TxShortFrameRetries	6
RxFailCnt	0

| [Home](#) | [Advanced setup](#) | [Exit](#) |

Network Configuration and Planning

Accton's Cheetah wireless solution supports a stand-alone wireless network configuration, as well as an integrated configuration with 10/100 Mbps Ethernet LANs.

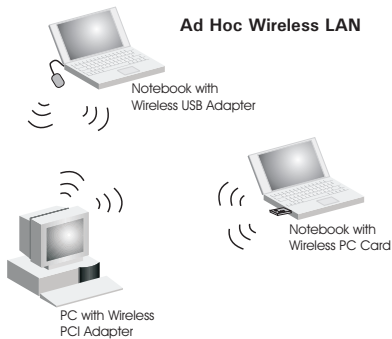
The Accton wireless network cards, adapters, access points and Wireless Access Point can be configured as:

- Ad hoc - for small groups that only communicate with each other
- Infrastructure - for wireless LANs
- Infrastructure wireless LAN - for roaming wireless PCs

Network Topologies

Ad Hoc Wireless LAN (no AP or Bridge)

An ad hoc wireless LAN consists of a group of computers, each equipped with a wireless adapter, connected via radio signals as an independent wireless LAN. Computers in a specific ad hoc wireless LAN must therefore be configured to the same radio channel. An ad hoc wireless LAN can be used in a SOHO or temporary environment.

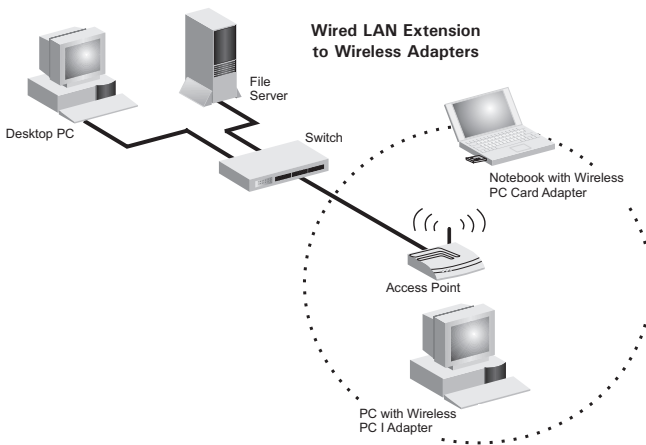


Infrastructure Wireless LAN

The WA5001 can also provide access to a wired LAN for wireless workstations. An integrated wired/wireless LAN is called an infrastructure configuration. A Basic Service Set (BSS) consists of a group of wireless PC users, and an access point that is directly connected to the wired LAN. Each wireless PC in this BSS can talk to any computer in its wireless group via a radio link, or access other computers or network resources in the wired LAN infrastructure via the access point.

The infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also increases the effective wireless transmission range for wireless PCs by passing their signal through one or more access points.

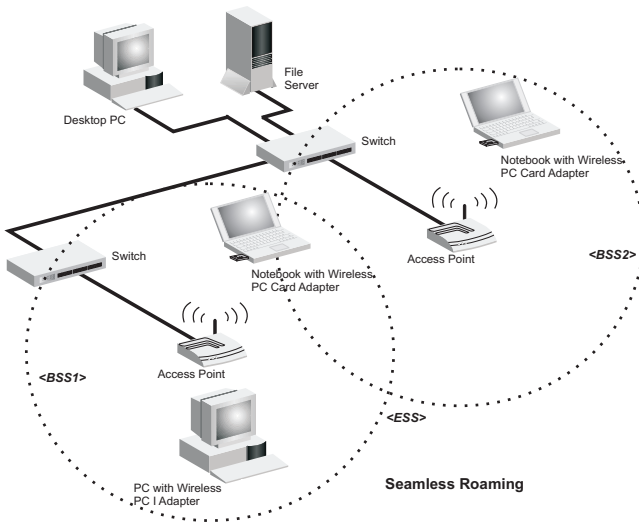
A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure.



Infrastructure Wireless LAN for Roaming Wireless PCs

The Basic Service Set (BSS) is the communications domain for each Wireless Access Point. For wireless PCs that do not need to support roaming, set the domain identifier (SSID) for the wireless card to the BSS ID of the access point to which you want to connect. Check with your administrator for the BSS ID of the access point or bridge to which he wants you to connect.

A wireless infrastructure can also support roaming for mobile workers. More than one access point can be configured to create an Extended Service Set (ESS). By placing the access points so that a continuous coverage area is created, wireless users within this ESS can roam freely. All Accton wireless network cards and adapters and WA5001 Wireless Access Points within a specific ESS must be configured with the same SSID.



Troubleshooting

Check the following items before you contact Accton Technical Support.

1. If mobile users do not have roaming access to the WA5001 Wireless Access Point, check the following:
 - Make sure that all the WA5001s and wireless devices in the ESS in which the WLAN mobile users can roam are configured to the same WEP setting, SSID, and authentication algorithm.

2. If the WA5001 cannot be configured using the Web browser (page 7):
 - Remove power from the WA5001.
 - Push in the reset button located on the back of the WA5001 to restore the factory default settings.
 - Plug the power connector back to the access point.

Accton Networks

802.11a Wireless Products Maximum Distance Table

Important Notice

Maximum distances posted below are actual tested distance thresholds. However, there are many variables such as barrier composition and construction and local environmental interference that may impact your actual distances and cause you to experience distance thresholds far lower than those we post below. If you have any questions or comments regarding the features or performance of this product, or if you would like information on our full line of wireless products, visit Accton's Website at www.acctontech.com

Accton 802.11a Wireless Products Maximum Distance Table									
	Speed and Distance Ranges								
Environmental Condition	72 Mbps	54 Mbps	48 Mbps	36 Mbps	24 Mbps	18 Mbps	12 Mbps	9 Mbps	6 Mbps
Outdoor Environment ¹	35 m (115 ft)	40 m (132 ft)	220 m (726 ft)	250 m (825 ft)	320 m (1056 ft)	350 m (1155 ft)	380 m (1254 ft)	450 m (1485 ft)	500 m (1650 ft)
Indoor Environment ²	12 m (40 ft)	18 m (60 ft)	25 m (82 ft)	30 m (99 ft)	35 m (115 ft)	40 m (132 ft)	45 m (149 ft)	48 m (157 ft)	50 m (165 ft)

- Notes:
1. Outdoor Environment: A line-of-sight environment with no interference or obstruction between access point and users.
 2. Indoor Environment: A typical office or home environment with floor to ceiling obstructions between access point and users.

Specifications

Physical Characteristics

Maximum Channels	US & Canada: 8 (normal mode), 3 (turbo mode) Japan: 5 (normal mode), 1 (turbo mode)
Maximum Clients	64
Operating Range	Up to 1,650 feet
Data Rate	Normal Mode: 6, 9, 12, 18, 24, 36, 48, 54 Mbps per channel Turbo Mode: 12, 18, 24, 36, 48, 72 Mbps per channel
Network Configuration	Infrastructure
Operating Frequency	5.15 ~ 5.25 GHz (lower band) US/Canada, Japan 5.25 ~ 5.35 GHz (middle band) US/Canada
LED Indicators	Power, Ethernet Link/Activity, Wireless Link/Activity
Power supply	Input: 100-240 AC, 50-60 Hz; Output: 3.3 V DC, 4 A DC
Output Power	16 dBm minimum
Physical Size	20.5 x 13.6 x 4 cm (8.07 x 5.35 x 1.58 in.)
Weight	280 grams (9.9 oz)
Temperature	Operating: 0 to 50 °C (32 to 122 °F) Storage: 0 to 70 °C (32 to 158 °F)
Humidity	5% to 95% (non-condensing)
Compliances	IEC 61000-4-2/3/4/6/11
Emissions	ETS 300 328 RCR STD-33A
Safety	CSA/NTRL (CSA 22.2 No. 950 & UL 1950) EN60950 (TUV/GS), IEC60950 (CB)
Standards	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.11a

Software Characteristics

Operating Systems	Windows 98/NT/2000/Me/XP
Network Management	HTML Web-browser interface, Windows 98/NT/2000/Me/XP utility

Sensitivity

Modulation/Rates	Sensitivity (dBm)
BPSK (6 Mbps)	-85
BPSK (9 Mbps)	-84
QPSK (12 Mbps)	-83
QPSK (18 Mbps)	-81
16 QAM (24 Mbps)	-78
16 QAM (36 Mbps)	-74
64 QAM (48 Mbps)	-69
64QAM (54 Mbps)	-65
BPSK Turbo (12 Mbps)	-82
BPSK Turbo (18 Mbps)	-81
QPSK Turbo (24 Mbps)	-80
QPSK Turbo (36 Mbps)	-78
16 QAM Turbo (48 Mbps)	-75
16 QAM Turbo (72 Mbps)	-71

Modulation

Modulation	5.15-5.25 GHZ (dBm)	5.25-5.35 GHZ (dBm)
BPSK (6 Mbps)	16	20
BPSK (9 Mbps)	16	20
QPSK (12 Mbps)	16	19
QPSK (18 Mbps)	16	19
16 QAM (24 Mbps)	16	18
16 QAM (36 Mbps)	16	18
64 QAM (48 Mbps)	16	16
64 QAM (64 Mbps)	14	14
BPSK Turbo (12 Mbps)	16	20
BPSK Turbo (18 Mbps)	16	20
QPSK Turbo (24 Mbps)	16	19
QPSK Turbo (36 Mbps)	16	19
16 QAM Turbo (48 Mbps)	16	18
16 QAM Turbo (72 Mbps)	16	18

Terminology

The following is a list of terminology that is used in this document.

Access Point — An internetworking device that seamlessly connects wired and wireless networks.

Ad Hoc — An ad hoc wireless LAN is a group of computers each with LAN adapters, connected as an independent wireless LAN.

Backbone — The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Base Station — In mobile telecommunications, a base station is the central radio transmitter/receiver that maintains communications with the mobile radiotelephone sets within its range. In cellular and personal communications applications, each cell or micro-cell has its own base station; each base station in turn is interconnected with other cells' bases.

BSS — BSS stands for "Basic Service Set." It is an access point and all the LAN PCs that are associated with it.

CSMA/CA — Carrier Sense Multiple Access with Collision Avoidance.

ESS — ESS (ESS-ID, SSID) stands for "Extended Service Set." More than one BSS is configured to become an Extended Service Set. LAN mobile users can roam between different BSSs in an ESS (ESS-ID, SSID).

Ethernet — A popular local area data communications network, which accepts transmission from computers and terminals. Ethernet operates on a 10 Mbps base band transmission rate, using a shielded coaxial cable or over shielded twisted pair wire.

Infrastructure — An integrated wireless and wired LAN is called an infrastructure configuration.

Roaming — A wireless LAN mobile user moves around an ESS and maintains a continuous connection to the Infrastructure network.

RTS Threshold — Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this "Hidden Node Problem." If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

WEP — Wired Equivalent Privacy is based on the use of 64-bit, 128-bit or 152-bit keys and the popular RC4 encryption algorithm.

WA5001
E042003-R01
150000007000A